NASA/KSC Secure Remote Access Services (SRAS) Account Request

KDP-P-3318

FOR INTERNAL USE ONLY Signed Request Form Received: _____ Tracking No: _____ Assigned Token S/N: _____

Instructions: Please read the following directions for completing this form. Requester: Complete Section A and review the "End User Agreement" before signing Section B. Section C and D must be signed by the appropriate individual before the internal approval process can begin. Requests missing the appropriate manager's signature will be returned to the requester. Deliver completed forms to the KSC Internal CSO listed in the CIO/CSO representative link https://itbs.its.ksc.nasa.gov/html/cio_cso_reps.html.

Section A END USER INFORMATION

Please complete all areas indicated below for requesting access to the Kennedy Secure Remote Access Services (SRAS). Use of this service is restricted to NASA and applicable contractors only. Access through SRAS is for U.S. Government Use Only. The SRAS Service is monitored. Unauthorized access to and/or use of this Network is a Violation of Law and Punishable Under the Provisions of 18 USC 1029, 18 USC 1030, and Other Applicable Statues.

First Name (as it appears on badge) _____ M.I. _____ Last Name _____ NASA Badge No. or X.500 ID _____

NASA Center _____ Building _____ Room _____ Mail Stop _____

Telephone _____ Email Address _____

IT Security Awareness Training Date _____ User Logon ID _____ NT Domain _____

Citizenship: ☐ U.S. Citizen ☐ Resident Alien ☐ Foreign National

Type of service required: ☐ Secure Remote Access Service (SRAS) ☐ Token Only ☐ Dial into KSC

This area is to be completed when the requester is issued a Token

Please provide three pass phrases: (Examples: What high school did you graduate from? "__", Favorite pet name? "__", Favorite snack? "__", etc.)

	Challenge Question	**Response**
1.		
2.		
3.		

JUSTIFICATION FOR ACCESS:

DURATION: Access will be valid for one calendar year. Re-submittal and justification will be required after 1 year.

REQUESTER'S EXTERNAL COMPUTER(s) ASSESSMENT CHECKLIST

In accessing your IT security risk use the following checklists to help determine your security environment:	**Yes**	**No**
1. Will a NASA provided computer be exclusively used with your SecurID Token?		
2. Will the computer being used with the account/service be used by anyone else (i.e., friends, relative, etc.) for unofficial purposes?		
3. Will you be utilizing a public computer (i.e., Library, Hotel, Motel, School, etc.) in conjunction with your Token?		
4. Will a current version of anti-virus software, scanning engine, and virus signature files be running on the computer?		
5. Are the anti-virus signature (pattern) files updated at least daily through an automated or manual process?		
6. Are software patches applied to the computer software, operating system, and applications on a regular basis?		
7. Are you aware or taking actions to avoid the dangers of email attachments and we browser spawned Trojans (spyware)?		
8. Will you be accessing ITAR or EAR information through your secure remote service?		

Section B END USER INFORMATION

KENNEDY SECURE REMOTE ACCESS SERVICES (SRAS)

Kennedy Secure Remote Access Services (SRAS) is the KSC system for off-site access to the KSC network. With limited exception, the system is for official Government business use only. The SRAS is a Centerwide resource, and users should immediately disconnect from the services when it is not actively in use. Those who misuse Government resources may face disciplinary action or prosecution as appropriate. The SRAS system is monitored and suspected misuse of Government-owned and/or provided data services will be referred to the Office of the Inspector General.

SRAS fall under guidelines and conditions of the NASA policies on "Appropriate Use of Computers and Networks."

The SRAS service provides a secure communication and authentication mechanism between remote hosts and the KSC Network perimeter. The protection of the information being accessed is the responsibility of the end user and the organization hosting the information. Approval of external access requests by the requester's manager, IT Security Office, and CSO signifies acceptance of any security risk associated with providing the external connectivity to the KSC Network environment.

REQUESTER'S ACCEPTANCE

I have read and accept the conditions of use associated with the requested access. I agree not to disclose any access information, personal access ID's, PIN, or passwords which are provided to me for access via the SRAS system. I understand the SecurID Token being issued is for my use exclusively. The Token is United States Government (NASA) property and upon my termination of employment or when the Token is no longer required, the Token will be returned to the KICS IT Security Office. If lost or stolen, I will contact the KICS IT Security Office immediately as I am accountable for all use of the Token and it's associated UserID. I also understand that this access will only be valid for one year from date of approval and a new request will be required for continued access. I hereby certify that the information provided is accurate to the best of my knowledge and belief.

Requester

Signature _____ Date _____

Section C REQUESTER'S MANAGER APPROVAL

APPROVAL: The following signature is required before the internal approval process can proceed. Requests missing the appropriate manager's signature can not be processed and will be returned to the requester.

I have examined the Requester's "End User Information" Section A for the described requested access and find the data to be accurate and justification adequate to approve the access request. I understand and accept the risk conditions of the "End User's Agreement" Section B. I agree to immediately notify KICS IT Security Office of employee's termination, **retirement**, or transfer to duties which no longer require remote access to perform assigned duties.

Requester's Manager

Printed Name _____ Organization/Mail Stop _____

Signature _____ Telephone _____ Date _____

Section D REQUESTER'S IT SECURITY OFFICE OR CSO APPROVAL

CIO/CSO representatives *https://itbs.its.ksc.nasa.gov/html/cio_cso_reps.html*

I have examined the Requester's "End User Information" Section A for the described requested access and find the security controls are adequate to approve the access request. Signature signifies acceptance of any security risk associated with providing the external connectivity to the KSC Network environment.

Requester's IT Security Office/Organization or CSO approval

Signature _____ Organization/Mail Stop _____ Date _____

Section E KSC INTERNAL CSO APPROVAL

CIO/CSO representatives *https://itbs.its.ksc.nasa.gov/html/cio_cso_reps.html*

I have examined the Requester's "End User Information" Section A for the described requested access and find the security controls are adequate to approve the access request. Signature signifies acceptance of any security risk associated with providing the external connectivity to the KSC Network environment.

Responsible NASA KSC CSO

Signature _____ Organization/Mail Stop _____ Date _____

Section F NETWORK CHANGE BOARD (NCB) APPROVAL

I have examined the Requester's "End User Information" Section A for the described requested access and find the security controls are adequate to approve the access request. Signature signifies acceptance of any security risk associated with providing the external connectivity to the KSC Network environment.

☐ Approved - KICS IT Security is directed to create the account, activate the access, or issue a SecurID Token as required.

☐ Denied (see comment)

Comment: _____

NCB Designee

Signature _____ Organization/Mail Stop _____ Date _____

Deliver signed form to the KICS IT Security Office; KICS-001, HQ Bldg. Room 1407.

Section G FOR KICS INTERNAL PROCESSING ONLY

KICS IT Security Office
(Sign when activated)

Signature _____ Telephone _____ Activation Date _____